LAPIN AMK
Lapland University of Applied Sciences

ALTERATION OF NETWORK INFRASTRUCTURE INCLUDING INFORMATION SECURITY
CASE: TAPOJÄRVI OY

Suvi Vähä

Bachelor's Thesis
Lapland University of Applied Sciences
Degree Programme in Business Information Technology

2015

LAPIN AMK
Lapland University of Applied Sciences

Abstract of Thesis

School of Business and Culture
Bachelor of Business Administration

Author Suvi Vähä Year 2015
Supervisor Sari Mattinen
Commissioned by Tapojärvi Oy
Title of Thesis Alteration of network infrastructure including information security Case: Tapojärvi Oy
No. of pages 51

The main objective of this thesis is to study the infrastructural alteration of a company network. The case company is a Finnish company Tapojärvi Oy. This thesis analyses the original network infrastructure, the requirements for the new one, the alteration, and finally it analyses the network infrastructure after the alteration. One objective is to study the information security of the network. Therefore, the thesis discusses the concept of information security and analyses the information security of Tapojärvi Oy's network.

Among several reasons, the growing number of employees in the case company resulted in a need for a change as the firewall encountered a massive load and ran out of capacity. The growth required a solution that enables a proper management for both users and network resources for flexible yet secure network. For an effective end solution, this thesis research uses empirical data generated on the field. The empirical data is supported by theoretical data from literature reviews.

The alteration included virtualizing the firewall and adding most of the sites logically in the same network although they physically remain in different networks. The VPN solution was changed from PPTP and IPSEC to SSL and some hardware was replaced.

The alteration of the network infrastructure resulted in a more secure, flexible, and liable network infrastructure. Furthermore, it led to a more user-friendly solution for remote users. This in conclusion influenced the business in a positive way, as a secure and functioning network is a business critical component for the case company.

Key words network infrastructure alteration, information security, data communication network

FIGURES AND TABLES

List of figures

List of tables

SYMBOLS AND ABBREVIATIONS

AP	Wireless Access Point
CA	Certification Authority
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
IMAP	Internet Message Access Protocol
POP	Post Office Protocol
SMTP	Simple Mail Transfer Protocol

ABSTRACT

FIGURES AND TABLES

SYMBOLS AND ABBREVIATIONS

CONTENTS

ACKNOWLEDGEMENTS

I would like to acknowledge the case company, Tapojärvi Oy, for commissioning my work. I hope this work can be used for further development in the ICT department of the company. My sincere gratitude to my boss, colleague, and a dear friend of mine, Arttu Iisalo, who has supported me, helped me, and encouraged me in my lowest moments. I will always remember your trust and faith in me.

Special thanks to my thesis supervisor, Sari Mattinen. Your patience helped me find the thesis subject of my interest, and your kindness and guidance has helped me from the first days as a student in Kemi-Tornio University of Applied Sciences to the last days in Lapland University of Applied Sciences. Thank you so much.

I would also like to thank all of my friends and my family. Special thanks to my siblings for their patience and faith in me. I would like to offer very special thanks to my parents who have emphasized the importance of education and allowed me to follow my dreams and more importantly, have always supported me. Finally, I would like to offer my gratitude to my former boss and a friend of mine, Antti Smeds, who emphasized the importance of finishing what you have started and whose kindness has helped me in many ways.

1 INTRODUCTION

1.1 Background and motivation

This thesis is made for Tapojärvi Oy, a Finnish mining and industrial company, with multiple sites around Finland. Tapojärvi Oy was established in 1955 and today the company is specialized in mining, factory services and material handling. The company employs around 370 people. Tapojärvi Oy is ISO 9001:2008 certified and its head office is located in Laivurinkatu in the center of Tornio. The sites are located around the whole of Finland and at the moment the biggest sites are in Kemi, Tornio, Raahe, Pampalo, Kylylahti and Kittilä in no specific order. (Tapojärvi, 2015.) Kittilä, Elijärvi in Kemi, Pampalo and Kylylahti are mining sites, and Raahe and Tornio steel works (hereinafter Röyttä) in Tornio are factory service units. In addition, Tapojärvi has a maintenance facility in Keminmaa and the management of maintenance is located in Oulunsalo. Tapojärvi Oy has an ICT department that consists of the ICT manager and the ICT coordinator. The ICT department is the main beneficiary of this work as this work will be a documentation of the alteration of the network infrastructure and can be utilized in the business continuity plan.

The servers of the company are located at the head office and the sites are dependable on them. Without access to the servers, the workers cannot record their working hours, which could result in delays in salary payment. Additionally, the maintenance database is on the server, and if the sites cannot access the database, they cannot record maintenance information of the vehicles on sites. Furthermore, if the sites are unable to access the servers, they are unable to access and record production data. Without production data, the company is unable to bill customers and without billing there will be no income. Therefore, as to many other companies today due to digitalization, a reliable and secure network and a secure and functioning virtual private network (hereinafter VPN) connection are vital for the company. As a growing company, the number of VPN users quickly grew which led to a massive load on the firewall. The increasing number of users was one of the reasons that created the need for an

infrastructural alteration of the network. This thesis researches the reasons why an alteration of the network infrastructure was needed and what was the outcome of the alteration. Furthermore, it researches the benefits of the alteration to the ICT department, end users, and to the company itself. It also focuses on the procedures of the alteration.

I started working at Tapojärvi Oy in April 2015 as the ICT coordinator. I participated in the alteration work of the network infrastructure, which was the main motivator for selecting this topic. Other motivator was the interest in networking and the desire to learn more about the topic from a security perspective.

1.2 Structure of the work

Chapter 1 is an introduction to this thesis work. It introduces the company and its business sites. Is also specifies the motivation for this work.

Chapter 2 discusses the research topic and methodology. More importantly, it discusses the research questions to which this thesis aims to answer.

Chapter 3 and 4 focus on theory. Chapter 3 explains the principles of data communication networks. It includes the discussion of topologies and security methods. Chapter 4 discusses the definition of information security.

Chapter 5 focuses on the network solution before the alteration of the infrastructure. It first discusses the networking solution, moving to discuss the solution at the head office. Furthermore, it concentrates on the problems of the original infrastructural solution, which were also the main factors that created the need for an alteration.

The chapters to follow discuss the comparison of different solutions as well as the analysis of the alteration. More specifically, chapter 6 discusses the planning phase of the alteration as well as the VPN solution, and chapter 7 discusses the

changes and consequences, as well as the benefits and problems of the alteration. Finally, the chapter provides information of the alteration of the network infrastructure on a site level.

Chapter 8 analyses the data communication network from an information security point of view. The final chapter provides the conclusion of the work.

2 OBJECTIVES, RESEARCH QUESTIONS AND METHODOLOGY

2.1 Research objectives

One of the objectives is to study Tapojärvi Oy's network. The study includes the original network infrastructure and the network infrastructure after the alteration. This objective focuses on the weak points of the original infrastructure, the requirements for the new one, the alteration, and the benefits and problems of the network infrastructure after the alteration.

Another objective is to evaluate the information security of the company's network. This objective includes the original network and the network after the alteration. The objective is to study how information security is applied in the network and what security policies and procedures are in use to ensure security of information.

2.2 Research questions

Three research questions are addressed in order to achieve the objectives of the research.

1. What were the factors that created the need for an alteration of the network infrastructure and how was the end solution selected?

The objective of this question is to study why the alteration was necessary. As the objective of the research is to study infrastructural change in the company, it is necessary to understand why a change that big was necessary. An infrastructural change has always impacts on the business and there are risks concerning it. By answering this question, the reasons for a change that big becomes clear. Furthermore, as usual, there are several solutions for problems. This question aims to explain why the specific solution was selected to be the solution for the problem.

2. What were the advantages and disadvantages of the alteration of the network infrastructure?

The objective of this question is to study the infrastructural network solution after the alteration and compare it to the original solution. The question seeks an answer to the question of what the benefits of the alteration were, as well as the problems and disadvantages. Hence, it analyses the results of the alteration.

3. How is information security applied in the network?

The objective of this question is to evaluate how the information is protected in the company. In order to answer this question, literature on information security are reviewed in order to be able to describe and explain the concept of information security. By answering this question, the analysis of the network infrastructure is supported from a security perspective.

2.3 Research methodology and methods

According to Collis and Hussey (2009, 73), a methodology is an approach to the research process and consists of different methods. Research data can be primary, meaning data from an original source, or secondary, meaning data from an existing source (Collis & Hussey 2009, 187).

The primary data on this thesis work is generated from me working at the company and being a part of the ICT department that executed the alteration of the network infrastructure. Hence, I am the collector of data. The research is therefore participant enquiry, which according to Collis and Hussey (2009, 80) involves the participants in the study that is conducted in a real scenario. In addition, the research is a case study meaning that it represents reality and gathers information in a natural setting to gain knowledge (Ellet 2007, 13) on a contemporary event (Yin 2009, 8).

Literature on data communication networks and information security were used for clarifying what a data communication network is, what it is used for, what it

includes, and to define what information security is. Literature on these topics were used to clarify the concepts and characteristics in order to be able to fully describe and explain the results of analysis.

2.4 Analyzing the data

Discussion and analyses of the primary and secondary data are conducted in order to find answers to the research questions and achieve the objectives of the thesis. The thesis work is a practical work and is based on empirical data generated from the field from participating in the alteration work. The empirical evidence is analyzed and the results of the analysis are reflected against the theoretical knowledge gained from relevant literature review in order to provide a comprehensive understanding of the topic for the reader. Furthermore, suggestions for further development are presented based on the results of the analysis.

From the case company's point of view, the outcome of these discussions and analyses will act as a foundation for the development of the network. The discussions and analyses ensure the information is documented and can be viewed and referred to. The discussions and analyses will act as part of the business continuity planning and ensure a more secure operation for the company. Finally, the discussions and analyses can be used in auditing.

2.5 Scope and limitation of the work

The scope of this work is to study the network infrastructure of Tapojärvi Oy. The focus is on those parts of the network where the biggest changes occurred while the alteration of the network infrastructure was executed. The work therefore is narrowed down to study the networking infrastructure, the head office in detail and in addition, one site.

Further, this research is narrowed down to focus on the aspect of a single user account. On sites, there are computers that are used by several different user

accounts. These computers need a VPN authentication certificate that is installed on the local device account of the computer and allows all users to use it. These certificates are very restricted. This work excludes these certificates and focuses on the certificates that are installed on the user accounts and can only be used by that user.

In addition, this research does not review literature on alteration of the network infrastructure, but focuses on information security literature and data communication networks literature. The reason for not reviewing literature on alteration of network infrastructure is that the solution for the alteration was especially tailored for the case company. Therefore, there is no relevant literature available as alterations of networks do not follow a general pattern. Further, this research will discuss technologies such as encryption technology in a general level as the technical details are irrelevant for understanding the topic as well as the analyses and discussion.

3 DATA COMMUNICATION NETWORKS

Fitzgerald (2007, 12) defines data communication as “the movement of computer information from one point to another by means of electrical or optical transmission systems” and refers to these systems as data communication networks. Data communication networks facilitate the daily businesses by offering faster transmission of data. (Fitzgerald 2007, 12.) According to Forouzan (2007, 7), a network is “a set of devices connected by communication links” and the purpose of networks is to transfer data from one point to another. He refers to this as “the basic concept of data communications” (2007, 1) and discusses about data communication between remote parties as networking. Forouzan provides a similar definition to data communication as Fitzgerald as he defines it as the “exchange of data between two devices via some form of transmission medium - -“(2007, 4). There are three main types of data communication networks: local area networks (hereinafter LANs), wide area networks (hereinafter WANs), and metropolitan area networks (hereinafter MANs). These networks differ in size and functionality. In some cases, a network can consist of LANs, WANs and MANs. An example of this kind of network is the Internet. LANs, WANs and MANs communicate through internetworking devices such as a router. (Forouzan 2007, 1-4.)

LAN, as its name specifies, is a small local network usually covering, for example, an office. A LAN can consist of either just a few devices or a variety of devices. The purpose of LANs is to share printers, data on a server, and other resources. LAN usually consists of a star, ring, or bus topology, which are discussed in detail later on this chapter. While LANs cover a small area, WANs enable long-distance data transmission. In other words, a WAN could cover a large area all the way from a country to the entire world. MAN is a size between LAN and WAN, and covers a city, or part of the city. (Fitzgerald 2007, 14-16; Forouzan 2007, 13-15.)

A data communication network consists of three different devices that are defined as basic hardware components of a network: a server that acts as a storage for data, a client such as a laptop that accesses the data on the server, and a circuit

such as a modem. Some networks, such as a home network usually do not have a server and neither needs one to function. In other words, even though a server is defined as a component of a network, it is not needed for the network to function. Company networks usually have a server, or several servers, that stores data and software applications. Data communication networks enable real time communication between devices all over the world. (Fitzgerald 2007, 12-13.)

According to Forouzan (2007, 4), a data communication network has four important characteristics: delivery, accuracy, timeliness, and jitter. These four components define the effectiveness of a network. Delivery means data is delivered only to the destination device. Accuracy refers to the correctness of data, meaning that it has not been changed during the transmission. Timeliness signifies the time during which a network transmits data. In other words, data has to be sent immediately so that the data stays up to date. The last character, jitter, refers to the variation of data transmission signals. For example, a video that is sent using uneven signals causes malfunction and uneven quality. Of these characteristics, timeliness and jitter relate to the performance of a network, which is one of the most important criteria of a network. Performance refers to the transmission time. In other words, it refers to the time it takes to transmit data from one device to another. The faster data travels, the better the performance of the network. Factors that influence on the performance include the number of devices, capabilities of the hardware, and the transmission medium. Another important criterion is the reliability of the network. This means the accuracy of delivery and the robustness of a network. Robustness signifies the ability to manage errors and abnormalities. Last important criteria is security. Security of a network refers to information security, which will be discussed in chapter 4, as well as protecting the network from viruses, intruders, and other factors that could jeopardize the functioning of the network. The security also refers to the ability to continue the network operation after a malfunction, intruder, virus, or other risk. (Forouzan 2007, 3-8.)

3.1 Topologies

Data communication network consists of devices that communicate with each other. In able to communicate, the devices have to be connected to one another. They can be connected either wirelessly or by wire, and be either a point-to-point connection or a multipoint connection. Point-to-point means two devices are connected to each other and the capacity of the communication link between them is used entirely for communication between those two devices. Multipoint connection means that there are more than two devices connected to one another and the capacity of links is shared. Topology refers to the layout of a network and represents how devices are interconnected. The topology can be physical representing how devices are physically installed and connected, or logical representing how the network conceptually works. The basic topologies are mesh, ring, star, and bus. The topologies are shown in figure 1 and are introduced under the bulleted headings below. (Fitzgerald 2007, 209; Forouzan 2007, 8-9.)

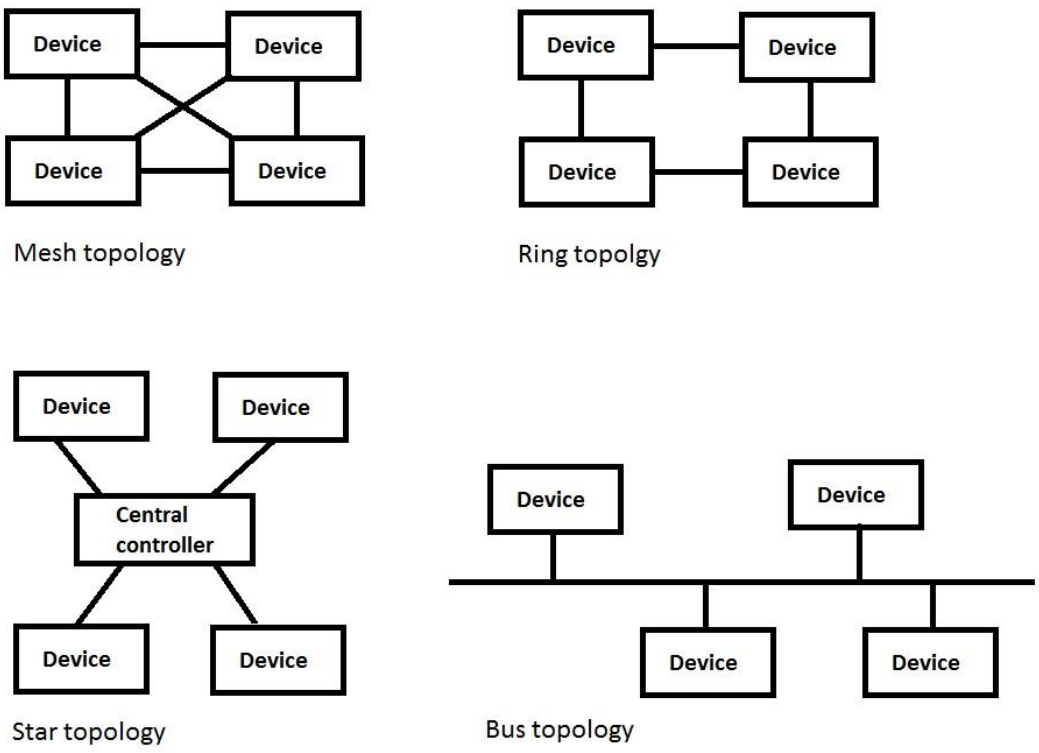

Figure 1. Network topologies

- Mesh topology

In a mesh topology, every device is connected to every other device over point-to-point links. The topology is robust; even if one device or link fails, the network will continue functioning through other links. In other words, there is no single point of failure. A disadvantage of the topology is that it can be very expensive and the implementation is demanding because all devices have to be connected to all other devices. (Ciccarelli *et al.* 2012, 146-148; Forouzan 2007, 9-10.)

- Star topology

In a star topology, every device is connected to a central controller, for example a router, over a point-to-point link. The devices are not directly connected to one another. The controller receives the traffic from the devices and directs the traffic to its correct destination. The topology is easy to install and even if one link fails, the other links are not affected. However, the controller is the central device in the topology and acts as a single point of failure, if it fails the entire network fails. (Ciccarelli *et al.* 2012, 143; Forouzan 2007, 10-11.)

- Ring topology

A ring topology, as its name specifies, is a ring where all devices are connected to the two devices on either side of it over point-to-point connections in a shape of a ring. A message travels along the ring to its correct destination. Ring topology is easy to install and faults are easy to detect. However, a fault in the ring can affect the whole network. As LANs today require a high transmission speed, the ring topology is rarely used, as it requires time for the message to move along the ring and find the correct destination device. (Ciccarelli *et al.* 2012, 141; Forouzan 2007, 12-13.)

- Bus topology

Whereas mesh, star and ring topologies uses point-to-point connections, bus topology uses a multipoint connection where all devices are connected to a long circuit. This circuit is the bus and is often referred to as a backbone. Once a device sends a message, it travels to the backbone and directs the message to

all devices attached to it. The Ethernet software on each device checks the address of the message and processes it only if it is intended to that device. The topology is easy to install, but the signal of the transmission gets weaker the longer it travels. Furthermore, faults are difficult to detect. (Ciccarelli *et al.* 2012, 136-137; Fitzgerald 2007, 209-210; Forouzan 2007, 11-12.)

To sum up, data communication networks are systems that enable the transmission of data between devices all over the world. They are used to exchange information and to transmit data in large volumes. The networks facilitate businesses as data is received and viewed as in real time. In other words, the data is up to date and business decisions are made based on that data. There are four main types of network topologies: mesh, ring, star, and bus. The topologies can represent the network either physically or logically.

3.2 VPN

VPN is a physically public, but virtually private network. It uses the data communication capabilities of an unsecured network but is secured by encryption protocols (Fitzgerald 2007, 322). A protocol is a set of rules used between devices in order for them to understand each other (Forouzan 2007, 19). A VPN encrypts the data in order to keep the content of the data private. The VPN also uses authentication of devices and users in order to prevent unauthorized user access. (Mattord &Whitman 2005, 274.) Sites and remote users use VPN to access the servers in a different network. A VPN software is installed on a device such as a laptop among with the user access rights. The VPN creates a private tunnel and through the VPN software, the user can access the servers remotely, for example, on a business trip. A VPN server such as a firewall supervises the VPN authentication. The VPN encryption protocols are discussed under the bulleted headings below. (Fitzgerald 2007, 322; Forouzan 2007, 1007.)

- PPTP

Point-to-point tunneling protocol (hereinafter PPTP) uses point-to-point protocol, which is a protocol that enables devices to dial up a point-to-point connection to

an Internet Service Provider (hereinafter ISP). PPTP uses the connection to ISP to create a private tunnel to another network, for example, a company's network. In PPTP, the encryption of data starts once the point-to-point connection to the ISP has been established. PPTP uses user level authentication and does not offer a very high security solution. In other words, PPTP does not authenticate the device. Today, PPTP is not a popularly used protocol due to lack of security. (Fitzgerald 2007, 137; Coca Jr., Gardinier, Morimoto, & Noel. 2004, 246-247.)

- IPSEC

IP security protocol (hereinafter IPSEC) uses a variety of encryption methods and operates either in transport mode or tunnel mode. Transport mode excludes the protection of the IP header and, therefore, does not protect the whole IP packet. The IP header contains information of the source IP address, destination IP address etc. Transport mode is used in a host-to-host connection. Tunnel mode protects the entire IP packet, including the IP header. Tunnel mode is used between two routers or between a router and a host. IPSEC uses authentication of both the user and the device. IPSEC encrypts data and every bite of the data has to be decrypted before the message can be seen. Therefore, the encryption and decryption of data in IPSEC requires an efficient processor, a large memory, and lots of capacity. While PPTP ensures only confidentiality of data, IPSEC ensure confidentiality, integrity, and reply protection. Confidentiality and integrity are discussed in chapter 4; reply protection refers to prevention of re-sending a stream. (Coca Jr., Gardinier, Morimoto, & Noel. 2004, 246-247; Fitzgerald 2007, 414; Forouzan 2007, 996-998.)

- SSL

Secure Socket Layer (hereinafter SSL) is an encryption protocol that offers a high security protecting the entire IP packet. As IPSEC, SSL also authenticates both the user and the device. Therefore, SSL and IPSEC both offer high security even though the implementation of the security is different. However, SSL requires less complex hardware configuration and capacity than IPSEC. (Andress 2014, 84-85; Forouzan 2007, 1008-1010.) SSL encryption is used on secure webpages

and one can notice the use of this encryption from the web address. An address without SSL encryption starts with *http://,* while and address with SSL encryption starts with *https://.* Further, SSL can be used to secure VPN connections. SSL in VPN uses CA certificate, which is a powerful, reliable, and secure authentication including information of the user and therefore verifying the identity of the user and ensuring the user is authorized. The certificates are so called digital signatures. A root CA offers certificates that not only authenticates the VPN users, but also authenticates the CA. For example, Sonera is a root CA meaning that the certificates offered by Sonera not only validates the user, but also validates Sonera as a root CA and ensures the certificate is real and authentic. Root CA certificates are extremely difficult to manipulate and fake and hence, the certificates offer a very high VPN authentication and connection solution. (Sullivan 2007, 19-22.) Finally, as IPSEC connects a network-to-network tunnel, SSL can be tailored to connect directly to a specific resource in the network, which increases security as the access is restricted (Andress 2014, 84-85).

4 INFORMATION SECURITY

Information security is a concept of protecting information. In the beginning, information security meant mostly providing a secure location for computers as the main threat was the theft of equipment. Information technology has, however, advanced greatly and today information security relies on the triangle of confidentiality, integrity and availability (hereinafter CIA). (Tipton & Krause 2008, 16.) International Organization for Standardization, commonly known as ISO, defines information security as the “preservation of confidentiality, integrity and availability of information” (ISO 2014). These three properties are seen in Figure 2, and is a common definition of information security.

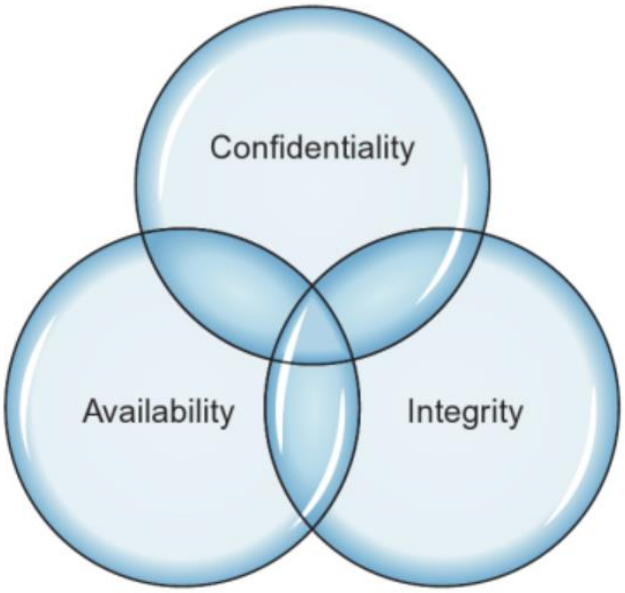

Figure 2. The CIA triad (Andress 2014, 5)

4.1 Confidentiality

In ISO/IEC 27000:2014(en) standard, which is a standard for information security management, ISO defines confidentiality as “property that information is not made available or disclosed to unauthorized individuals, entities, or processes” (ISO 2014). According to Greene (2006, 67), confidentiality aims to “prevent the unauthorized disclosure of sensitive information”. In her opinion, however, there are several threats for confidentiality. These threats include hackers, applications

that can crack passwords, malicious code such as viruses and Trojan horses, unauthorized user activity, and shoulder surfing (Greene 2006, 68). Shoulder surfing refers to looking at another person's computer monitor and the information on it and is a very common threat for confidentiality as one can simply not notice this happening, or it could be a result of trust. However, several procedures and solutions can mitigate and prevent these threats. These procedures include, for example, access control, backup, firewalls, antivirus, and VPN. (Greene 2006, 67-68.)

In sum, confidentiality is an essential property in all security matters and can be applied in several levels. For example, in a company confidentiality means that information is not trusted to everyone. User accounts are configured with the correct and restricted access rights. All critical information is kept secured and unauthorized access is denied. The users have user accounts secured by passwords and the ICT department ensures users are allowed to access only the information that is necessary for them and not more. In other words, the company seeks to avoid security breaches that could have serious consequences.

4.2 Integrity

According to ISO (2014) integrity refers to the protection of the accuracy and completeness of assets such as data. Greene (2006, 69) provides a similar definition to the concept as she defines integrity as "the protection of system information or processes from intentional or accidental unauthorized modification" (2006, 69). Integrity represents the correctness of data, meaning that there has been no deletion of data, or undesirable modification in the data, even if it was a small modification. (Greene 2006, 69-70.) According to Andress (2014, 6-7), integrity does not only mean protecting information from unauthorized modification, but also from authorized undesirable modification. He also states that the concept is not just about preventing these changes, but also about having a solution to undo these changes by trained, authorized users (Andress 2014, 6-7). Given these definitions of data integrity, it can be stated that integrity is closely related to access control. ISO (2014) defines access control

as a “means to ensure that access to assets is authorized and restricted based on business and security requirements”. Even though integrity and access control concepts are similar to each other, they still have different definitions and should not be confused with each other.

In Greene’s perception, the threats for integrity are more or less the same as for confidentiality. In other words, Greene lists hackers, malicious code and unauthorized user activity as integrity threats, but adds interception and alteration of data transmission to the list. (Greene 2006, 69-70.)

In summary, integrity means that no authorized nor unauthorized, intentional nor unintentional changes that represent false information have been made. Integrity reflects the level to which information represents reality.

4.3 Availability

ISO (2014) defines availability as “property of being accessible and usable upon demand by an authorized entity”. In other words, it means that data is accessible whenever it is needed. ISPs and their customers have signed a Service Level Agreement, which specifically states an uptime of 99.999%. This means that all information is available 99.999% of the time as well. Availability means that when the user wants and/or needs to access information, the information is available and accessible. Many business decisions are made based on the data and therefore, in order to keep the business running, the data has to be available upon demand. (Greene 2006, 69-71.)

There are threats for this property of the triad as well. Threats that could result in data not being accessible could be software problems, hardware failure, power loss, natural disasters, man-made error, and as for confidentiality and integrity, malicious code. (Greene 2006, 70-71.) Furthermore, a loss of availability may occur as a result of an attacker. An attacker is someone unauthorized and a loss of availability caused by this kind of outside party is called Denial of Service, also known as DoS. (Andress 2014, 7.)

When designing information security policies, availability is often given less attention than confidentiality or integrity. However, availability threats are likely to happen at one point or another as hardware, for example, will not be up and running forever. It will fail eventually. Nevertheless, there are standard controls to prevent the loss of availability. These include, for example, backups, redundant databases, Uninterruptible Power Supplies, commonly known as UPS, and air-conditioning. (Greene 2006, 71-72.)

To sum up, availability refers to data being accessible to authorized users whenever and wherever needed. It is difficult to verify which property of the CIA triad is the most important, or whether they all are equally important. The importance depends a lot on the organization. On one hand, one may argue that availability is the most important property because it does not matter whether information is confidential or has integrity, if it is not available. On the other hand, a question arises what one does with the information that has no integrity and cannot be trusted to represent reality, or with such information that is not kept confidential. These three properties are all essential for information to be secure and combined with a secure physical location and trained personnel can provide a very effective security solution. (Greene 2006, 71-72.)

5 ANALYSIS OF ORIGINAL INFRASTRUCTURE

5.1 Original network infrastructure

Around 8 years ago, Tapojärvi's networking solution changed from Corporate Access Network (hereinafter CAN), to a solution that is illustrated in figure 3. The change was necessary because it was not possible to have mobile networks in CAN. Furthermore, VPN solution in CAN was extremely expensive and only available for purchase in 5-piece sets. Tapojärvi had two sets and the VPN connection was only installed in one computer at each site. To only have a VPN connection in one computer on each site with several users was troublesome and a non-user-friendly solution. Therefore, the CAN solution was cancelled.

The networking solution after CAN included an in-house firewall that was called Kerberos. VPN worked mostly through PPTP, but some connections were using IPSEC protocol. The firewall was located at the head office, which is located in the center of Tornio. In this office, staircase C, are located all the servers and several departments including accounting and salary calculation. There is another office in the same building in staircase B where the ICT and Human resources departments are located. In this thesis, the head office in staircase C is referred to as head office C, and the head office in staircase B is referred to as head office B.

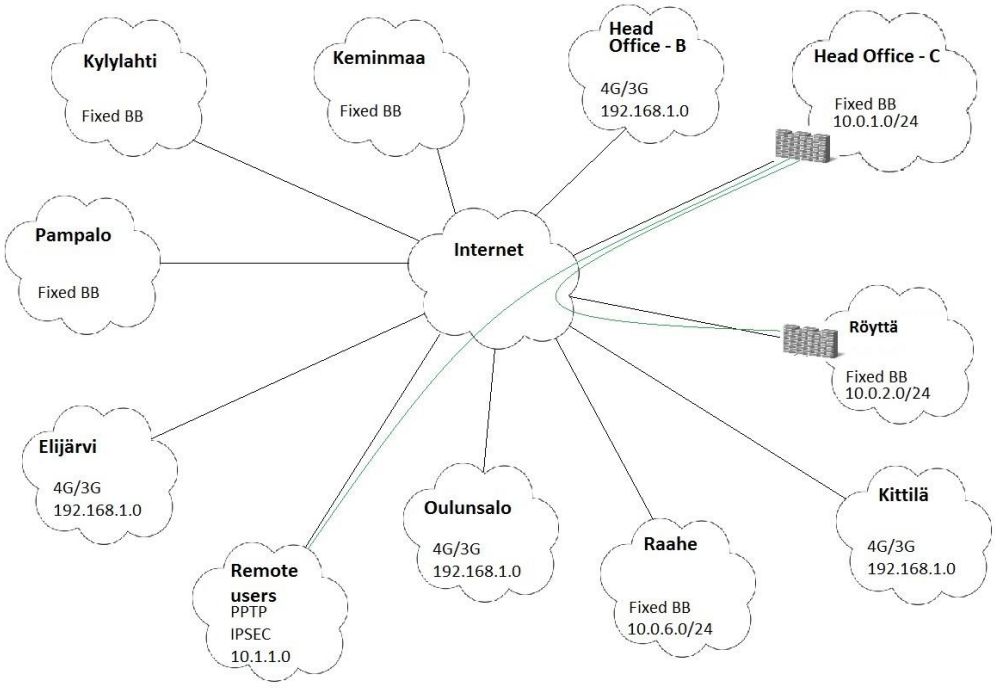

Figure 3. Networking infrastructure before the alteration

Head office C and Röyttä had fixed broadband (hereinafter fixed BB) connections with address 10.0.1.0/24 at the head office C and 10.0.2.0/24 at Röyttä respectively. They were connected through fixed IPSEC VPN. Remote users were connected through VPN using 10.1.1.0 addressing. The green lines in figure 3 illustrates that remote users were able to connect to the head office C and that head office C and Röyttä were connected to each other. Remote users were also able to connect to Röyttä, but the traffic went through the firewall at the head office C. Röyttä had an in-house firewall as well. However, the outgoing traffic from Röyttä went to head office C before it was directed to its correct destination. This was because Röyttä used the server Apollo as the DNS server. The incoming traffic to Röyttä, however, was configured to move directly to Röyttä without going through head office C. The firewall in Röyttä controlled the incoming traffic.

Kylylahti and Pampalo uses a third party fixed BB connection. Keminmaa used Sonera company Internet fixed BB connection. Head office B, Kittilä, Oulunsalo, and Elijärvi used Soneras' consumer level 3G/4G connection and consumer level

routers. As seen in figure 3, Raahe used 10.0.6.0/24 addressing, but the fixed BB was a third party connection and was not part of the same core network with head office C and Röyttä. The same site-to-site IPSEC VPN connection that was between head office C and Röyttä was once tested with other sites as well. However, the VPN tunnels did not stay up due to the poor quality of connections and insufficiency of devices.

Kerberos had a terrific reporting system; the ICT department was able to see real time information of the network traffic on a packet level. Due to the specific reporting, causes of problems were easy to diagnose. Figure 4 illustrates the original infrastructure at the head office C LAN before the alteration of the network infrastructure occurred. Head office C uses 10.0.1.0/24 network.

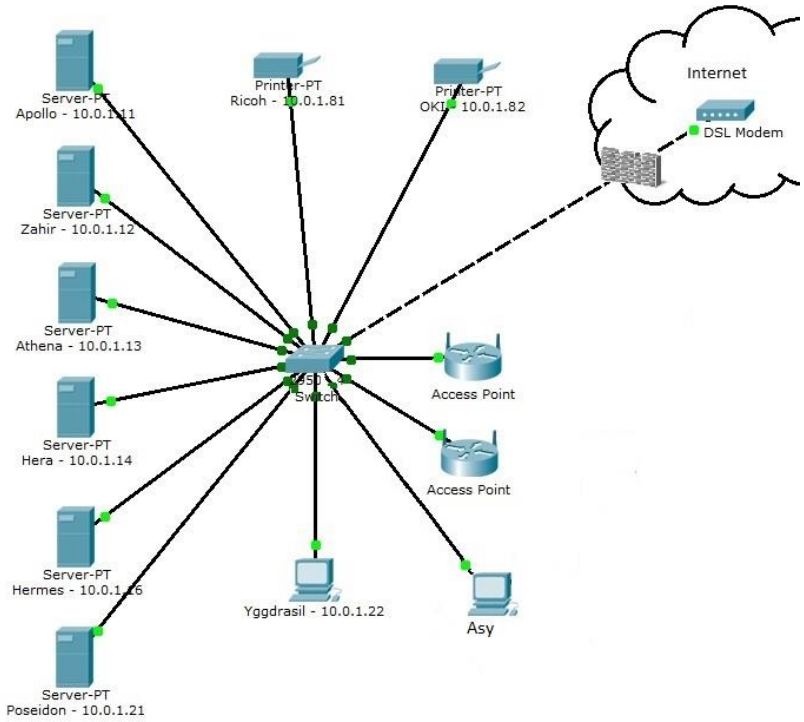

Figure 4. Head office C LAN infrastructure before the alteration

The firewall Kerberos was located in-house between the switch and the DSL modem. The office had two printers: Ricoh upstairs and OKI downstairs. The office also had two access points, and the backup system Yggdrasil with an IP

address of 10.0.1.22. Asyniur, an automatic system that sends email notifications and reports was also located at the head office C. The head office C LAN used star topology. Even though the physical implementation located the switch as the central controller (figure 4), the firewall was logically the central controller of the network as it worked as the DHCP server and directed the traffic to its correct destination. For clarity, employees' end devices are not shown in figure 4. Employees used the DHCP pool for IP addressing and were connected wirelessly and by wire.

5.2 Reasons for alteration

In spring 2014, the first symptoms manifested themselves. Users started to complain that the VPN crashed, could not be connected, and was extremely slow. The cause of these hitches was that the number of remote users started to exceed the capacity of the firewall. The idea of making changes in the network infrastructure had been in mind before, but this was the first time problems occurred and the need for an alteration became topical. Below in bulleted headings are listed reasons and shortages that resulted in the alteration of the network infrastructure. At the same time, the correction of these shortcomings became the requirements for the new network infrastructure.

- Increasing number of personnel

Tapojärvi Oy is a quickly growing company. According to Tapojärvi Oy's Human Resource plan 2015, there were 33 employees working in the company in 2003. In 2010, there were 191 employees and in 2015, there are 376 employees. Figure 5 illustrates the total number of employees during years 2003 to 2015.

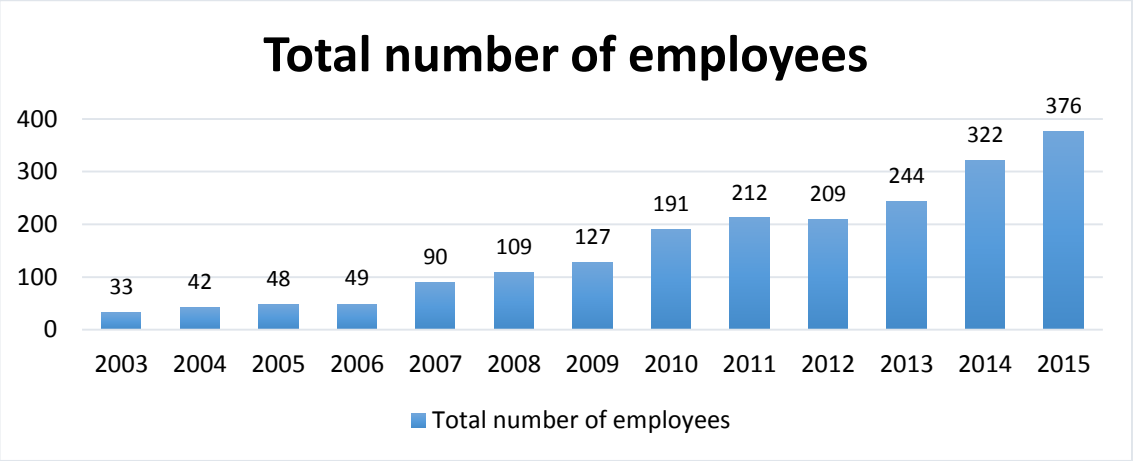

Figure 5. Total number of employees (Tapojärvi 2015)

The total number of employees has grown each year, except for in 2012 when it dropped by three employees. Since then, the number of employees has grown again.

According to the human resource plan 2015, most employees work outside the head office. Figure 6 illustrates the percentage of employees by sites.

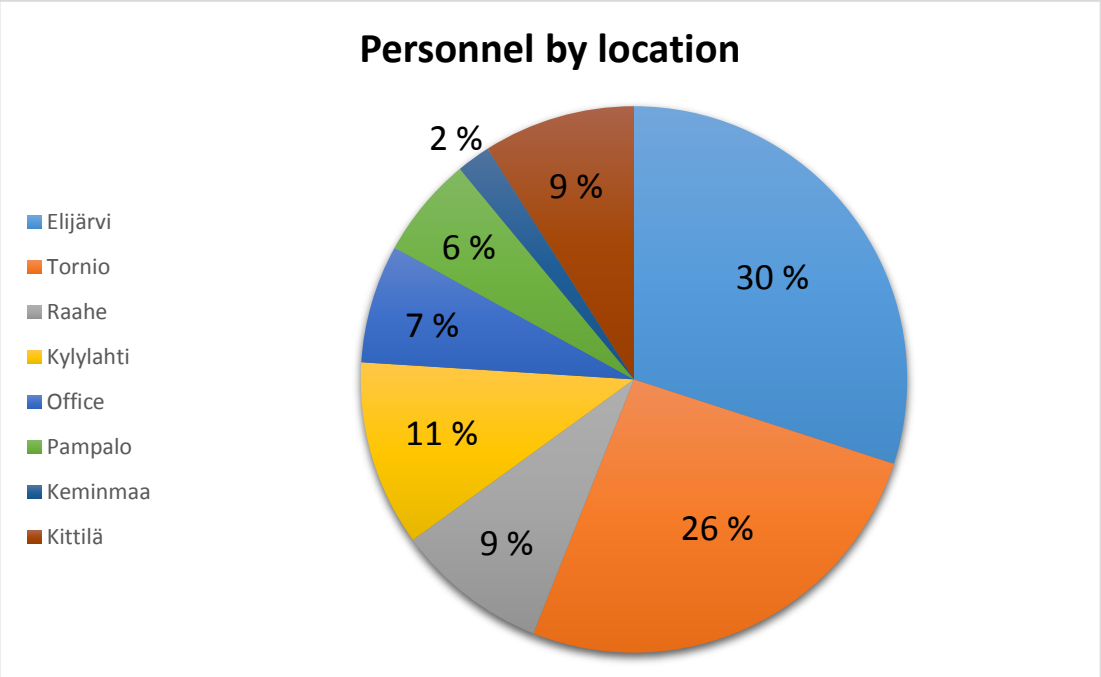

Figure 6. Personnel by location

In 2015, only 7% of the employees work at the office. This means that 93% of the employees work outside the office and need a VPN connection for remote access. The number has increased from 2014, but even then, the majority of employees were located outside the office. This fast increase in the number of employees and, therefore, in devices such as desktops and laptops was one of the main reasons for a need for an alteration. Kerberos could not handle the amount of traffic. Furthermore, the firewall Kerberos was several years old; even if the number of employees had not increased, a change would have been necessary at one point. As was discussed in subchapter 4.3, the hardware will not last forever and in order for the information to stay available, it is necessary to ensure hardware does not exceed its capability. Nevertheless, the number of personnel was increasing continuously and hence, the problem was not solved.

Once the problems of firewall exceeding its capacity started, more VPN connections were changed from PPTP to IPSEC. As discussed in subchapter 3.2, PPTP does not offer a very high security, and therefore IPSEC with an increased security level engaged attention of the ICT department. However, the penetration and processor capability of Kerberos was not sufficient for IPSEC. As discussed in subchapter 3.2, IPSEC demands a lot from the firewalls processor and memory in able to handle the incoming packets that Kerberos was not powerful enough.

- Power outages

Another thing that caused problems were the power outages. Once the head office faced a power outage, Röyttä lost its Internet connection as the server Apollo 10.0.1.11 at the head office C was the DNS server. The firewall distributing the DHCP pool of the DNS server disoriented the access to Apollo.

- Lack of domain connections

A domain connection means the end device is on the domain area, or it has a VPN connection where the network is physically outside the domain but logically in the domain area. The original networking infrastructure had a domain

connection only at the head office C and in Röyttä. For example, it was not possible to access the security cameras at Röyttä on 10.0.2.0/24 from Elijärvi 192.168.1.0. It was only possible as a remote user but even then, it was not possible without going through Kerberos at head office C. This was troublesome and one area that needed a change. In addition, without domain connections, there was a lack of information security. All user accounts are members of the domain tapojarvi.local and have access to servers with the access limited by access rights. If rights had to be taken away from a user or the user account had to be disabled, the disabling or the new access rights would not be valid until the user connectes to the domain and the new rules are inherited. This means the user had to connect over the VPN or physically be at the head office C and connected to the domain. Hypothetically, if a device was stolen and the password was cracked, an outsider could have accessed confidential information and the disabling of account would not take place until a connection to the domain was established. Considering the definition of information security: confidentiality, integrity, and availability, the first two mentioned was jeopardized.

- Lack of centralized WLAN management

As discussed earlier in subchapter 5.1, many sites used consumer level devices and connections. Huawei B593S router was one of the consumer level devices in use, but there were also other devices from other manufacturers such as Zyxel. As there was no corporate solution with corporate level devices and connections, there were many problems with wireless LAN, commonly known as WLAN, and the Internet connection itself. Furthermore, there was no WLAN controller where all the WLANs could be managed.

Finally, the ICT department wanted to outsource the maintenance and administration of the firewall. This, and all reasons discussed above were factors that created the need and process for an alteration of the network infrastructure.

6 PLANNING AND EXECUTING THE ALTERATION

6.1 Comparing solutions

The change started with realizing the problem. After realizing the problem, a solution that responded to Tapojärvi Oy's needs was necessary. One option could have been buying a new firewall. Several firewalls and firewall solutions were compared. Properties that were focused on were the security, capacity, support, price, and manageability. However, a firewall that could have responded to company needs would have been so expensive that the option of buying a new firewall was excluded. In addition, a new firewall would have required a broadband speed that is not available for the location. The resources were insufficient and therefore the solution was not profitable. Furthermore, buying a new firewall would have only solved one problem of many.

Another option was to outsource the maintenance of the firewall. The burden of Tapojärvis' ICT department of being the sole administrator of the firewall would have been evaded. The problem was that local companies did not have enough experience nor knowledge to manage the outsourcing of the firewall and therefore were not trusted and the option was excluded. In addition, outsourcing the physical firewall would not have solved all problems.

As discussed earlier, Tapojärvi used to have CAN solution. Sonera offered the CAN solution. This means the cooperation with the tele operator company Sonera has been valid for years. Sonera currently offers mobile subscriptions and many other company solutions for Tapojärvi. Therefore, it was only natural to approach Sonera with the problem in hand and ask for a solution.

6.2 Negotiation with Sonera

To get to a solution that satisfied both parties was not easy. Tapojärvi Oy first told about the problem and a desirable solution, which included deleting the problems of the network infrastructure shortages discussed in subchapter 5.2. Sonera

offered CAN for the solution, but after already having first-hand experience and knowledge of it, Tapojärvi Oy was wise enough to decline. The discussion of what the customer wished for and what the tele operator company offered went on for a whole year. Finally, the solution of a virtual firewall came up after Sonera had had a similar case with another company. The problem was the price that had to be renegotiated. The price of the solution is not mentioned in this thesis because of the confidentiality of the document and irrelevancy for this thesis work.

Once both Tapojärvi and Sonera agreed on the solution and the price, a preparation and execution plan was made. This plan included risk assessment; what could go wrong during the alteration, what consequences does it have, what regulations and exceptions has to be taken into consideration etc. After all the paperwork was finalized, a date for the alteration had to be decided. The alteration had to occur in a time that would have a minimal impact on the business. With a company that has several sites working 24/7 all around Finland, this was not an easy task. An assessment of parts of the business that cannot be interrupted and that cannot handle the system going down was essential as the alteration concerned an infrastructural alteration. These parts are salary calculation, accounting, and billing on sites. In addition, all other big exceptions and occurrences on sites were taken into consideration.

6.3 The VPN solution

The alteration of the network included changing the VPN from PPTP and IPSEC to SSL VPN. The VPN authentication was implemented through a root certificate offered by Sonera. Tapojärvi wanted a user-friendly solution where the user does not need to enter the password every time the user connects the VPN. Yet, the solution had to be secure. As was discussed in subchapter 3.2, Sonera is a root CA and therefore the certificates offered are extremely secure. How the certificate authentication of Soneras' full SSL VPN authentication functions is that, the certificate is installed on the local user account on each computer and when establishing a VPN connection the certificate is authenticated and then the certificate authenticates the user. The certificates are personal, and the user

profile of each certificate specifies the access rights of the user when using VPN connection. The certificates are created in a secure portal by the ICT department of Tapojärvi Oy. In the portal, the user profiles can easily be managed, modified and, if necessary, deleted. The deletion of user profile ensures the user cannot establish a VPN connection.

On a security matter, the change from PPTP and IPSEC to SSL was a positive thing as the SSL is more secure than PPTP, and requires a less complex configuration than IPSEC as discussed in subchapter 3.2. The VPN software solution will be discussed in more detail in the next subchapter.

In sum, the requirements for the new network infrastructure were domain connections, centralized WLAN management, higher security level, and decreased number of VPN remote users. An additional requirement was removing the problem of Röyttä losing Internet connection when the head office has a power outage. The solution offered by Sonera was the virtualization of the firewall and SSL VPN with certificate authentication.

6.4 The alteration of the network infrastructure

Phase 1: switching the firewall

The alteration started by Sonera redirecting the network traffic. They redirected both the outgoing and incoming traffic from and on Tapojärvi Oy's IP addresses to the virtual firewall on the Internet. This was basic administration of Soneras' network. After redirecting the traffic, they turned on the virtual firewall among its regulations.

At this point, it was Tapojärvi Oy's turn to turn off the Kerberos firewall in-house and connect the network cable from the old firewall to the nearest local network switch. This enabled the traffic to access the core network. Once the old firewall was turned off and the new one was turned on, it was time to test the network connection at the Head office C. The connection worked although there was

some minor errors with the DNS server. This error is discussed more on the subchapter 7.2.

The next step was to shut down the in-house firewall at Röyttä. This was made the same way as at the head office; the firewall was turned off and taken away and the network cable that used to be connected to the firewall was connected directly to the switch.

Phase 2: installation of VPN

After the firewall was virtualized, the installation of VPN on remote user's computers started. The goal was to install as many as possible in a time as short as possible. The installation went forward according to priority and included the installation of Junos Pulse and the certificate. Junos Pulse is a VPN software that creates a secure VPN tunnel. It starts up automatically in places it is needed. Hence, Junos Pulse works in a user-friendly manner where the user does not have to set up the VPN manually. The VPN connection is automatically established once the device is connected to the Internet. This is, if the user has an valid certificate.

The first step in the installation process was to add the installation packet and the preconfigured installation command to C:\Temp folder and then run the command as administrator. The installations occurred both locally and through remote access to users computers. Second step on the installation process was to install the client certificate. For this, the ICT department created remote user accounts at Soneras' secure manager portal. Secure manager portal is the administration tool for the VPN user accounts. Installation link to activate the preconfigured accounts were sent to users email address and the ICT department was responsible for installing the certificate on the local user account. Figure 7 illustrates a connected and functioning VPN software and client certificate installation.

Figure 7. Illustration of a functioning VPN connection

If the installation was not successful, the VPN would be disconnected and an error message of ‘Invalid or missing client certificate’ would be displayed. The installation of the VPN was very straightforward and unsuccessful installations were easy to notice.

7 ANALYSIS OF THE ALTERATION

Figure 8 illustrates Tapojärvi Oy's networking infrastructure after the alteration.

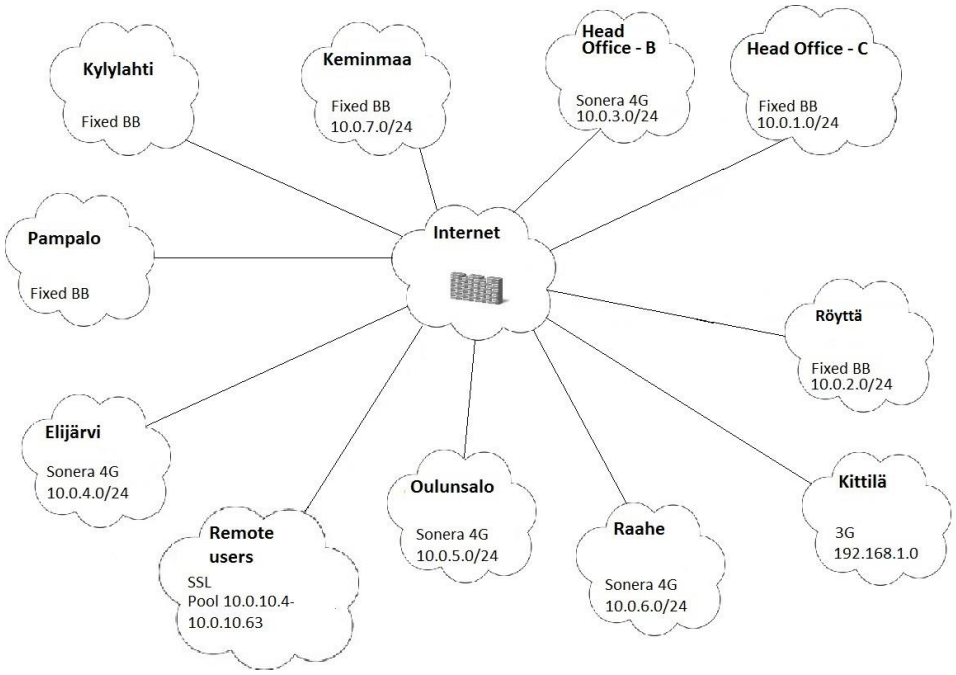

Figure 8. Networking infrastructure after the alteration

The most significant change was the change of the physical firewall at head office C to a virtual one on the Internet. The virtual firewall enabled the regional offices to be connected to each other's and to the head office, as they are subnets of the same core network. The subnets therefore form a fully functioning WAN. The IP addressing at head office C and Röyttä stayed the same. Head office B, Elijärvi, Oulunsalo and Raahe had Cisco 810 series corporate level 4G modems and 4G connections installed with subnet IP addressing 10.0.3.0/24, 10.0.4.0/24, 10.0.5.0/24 and 10.0.6.0/24 respectively. Keminmaa experienced a change of Sonera corporate Internet into Sonera coporate Internet plus which is a faster connection and enabled the IP addressing to be changed to 10.0.7.0/24. Kylylahti, Pampalo and Kittilä stayed the same due to lack of 4G network in the areas. These sites depend on SSL VPN. Remote users use the pool 10.0.10.4-10.0.10.63. The WAN topology represents an extended star topology, although AP devices have capabilities to a mesh topology. Extended star topology means that the virtual firewall acts as the central controller in the WAN that directs the

data to its correct destination site and each site LAN uses a star topology where the router acts as the central controller. In other words, an extended star topology means that the WAN uses star topology and in addition, all LANs in the WAN use star topology. The virtual firewall and the router on each site, therefore, act as the single point of failures in the networks.

7.1 Benefits of the alteration

One of the benefits of the alteration was the outsourcing of the firewall and its maintenance. Today, Tapojärvi's ICT department is not the sole administrator of the firewall, which was a huge relief. Sonera administrates the firewall as well which means that the respond time to any problem has therefore significantly decreased.

Another benefit was the reduced number of remote users as the users at the head office B and C, Keminmaa, Elijärvi, Oulunsalo, Raahe, and Röyttä do not have to connect through Junos Pulse VPN, but are connected as part of the same core network. As was discussed in subchapter 5.1, during the old solution if the remote users wanted to connect to Röyttä, the traffic went first to the firewall at the head office C after which it was directed to Röyttä. Today with the virtual firewall, the traffic is not directed through head office C but instead moves directly to Röyttä. With sites existing on the same core network, it is now possible to access the cameras at Röyttä from the mine in Elijärvi. Such access was not possible before.

Furthermore, among the benefits was that the management of printers is now centralized at the server. Before the alteration, the installation of a printer included installing the driver first, and then the printer. There were three different options for installing the driver: the driver was on a USB stick, it was sent remotely, or it was downloaded from the Internet. Today, as the printer is installed and managed at the server, the printer can be directly installed in the control panel and the installation process automatically includes the installation of a printer driver.

In addition, a benefit of the alteration was that the WLAN signal strength and management of WLANs improved. WLAN was a weak point of the company and was a constant target of complaints, mainly caused by the devices. There were many different devices in use and they were all consumer level devices. There was no controller managing the WLANs. After the alteration of the network, a controller named Hercules was added to the infrastructure. Hercules is a wireless LAN controller, Ruckus ZD1200, which allows robust management of networks. Tapojärvi Oy has licenses for ten APs of which nine are in use. These APs are managed from Hercules and are listed in table 1 providing the device name, location, model, status, and IP address.

Table 1. Active APs

Device Name	**Location**	**Model**	**Status**	**IP address**
LaivurinkatuCAP	Head office C	r500	Connected	10.0.1.31
RoyttaAP1	Roytta, upstairs	r500	Connected	10.0.2.30
RoyttaAP2	Roytta, downstairs	r500	Connected	10.0.2.31
LaivurinkatuBAP	Head office B	r500	Connected	10.0.3.30
ElijarviAP	Elijarvi on surface	r500	Connected	10.0.4.30
OulunsaloAP	Oulusalo	r500	Connected	10.0.5.30
RaaheAP	Raahe depot	r500	Connected	10.0.6.30
KmaaAP1	Keminmaa upstairs	r500	Connected	10.0.7.30
KmaaAP2	Keminmaa downstairs	r500	Connected	10.0.7.31

Hercules offers a flexible management of WLANs. All access points have two WLANs: one for the employees named TAPWLAN, and one for the guests named TAPGUEST. Before the alteration, the head office C was the only place with a guest WLAN. Hercules also provides specific information of the WLANs active clients as seen in figure 9.

Active Clients

OS/Type	Host Name	User/IP	Role	Access Point	WLAN	Radio	Signal (%)	Status	Auth
Windows 7/Vista	EFL55JMA	10.0.3.228		Laivurinkatu B	TAPWLAN	802.11a/n	99%	Authorized	OPEN
Windows 7/Vista	TapLehtola2014	10.0.2.105		Roytta ds	TAPWLAN	802.11a/n/ac	64%	Authorized	OPEN
Windows 7/Vista	Tuntilap-KKT3	10.0.2.131		Roytta us	TAPWLAN	802.11b/g/n	79%	Authorized	OPEN
Android	android-bf6a89f54883bbd	10.0.4.152		Elijarvi	TAPWLAN	802.11b/g/n	79%	Authorized	OPEN
Windows 7/Vista	RaahTlappu1	10.0.6.105		Raahe	TAPWLAN	802.11b/g/n	84%	Authorized	OPEN
Windows 7/Vista	TapFeCr-2012-Tomi	10.0.2.120		Roytta ds	TAPWLAN	802.11a/n	64%	Authorized	OPEN
Windows 7/Vista	TapPetteri	10.0.2.145		Roytta us	TAPWLAN	802.11b/g	99%	Authorized	OPEN
Windows 7/Vista	Elij-tuntilap-1	10.0.4.110		Elijarvi	TAPWLAN	802.11b/g/n	62%	Authorized	OPEN

Figure 9. View of active clients on WLAN controller

It shows the operating system, host name, IP address, which access point is it using and so on. Most importantly, it shows the signal strength, which makes it easier for the ICT department to manage the WLANs and provide a functioning Internet connection, which is vital for the business operations. After the alteration of the network infrastructure and addition of Ruckus controller and access points, there has been no complaints about the Wireless network not working. A problem that used to occur daily was removed. Furthermore, Hercules offers event log that provides information on new and disconnected rogues. Suspicious devices can be blocked from the controller. It is easy to monitor the rogues on all the sites with an AP, which means the majority of the company. Hercules and LaivurinkatuCAP access point are seen in figure 10, which illustrates the LAN network infrastructure at the head office C after the alteration.

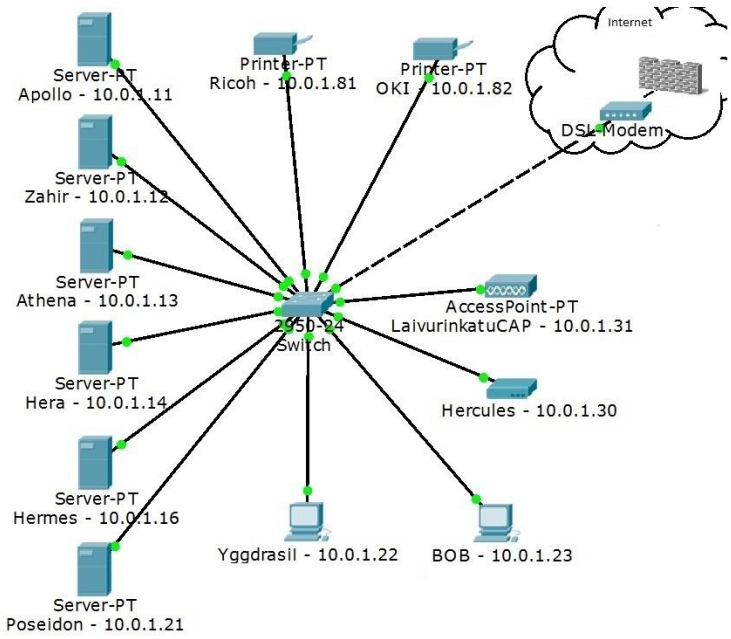

Figure 10. Head office C LAN infrastructure after the alteration

When comparing the old solution (figure 4) and the new solution (figure 10) one can notice that the firewall and DSL modem have changed places. The virtual firewall managed by Sonera is on the Internet. The servers and printers have stayed the same. The backup station Yggdrasil has also stayed the same but is no longer the only backup station. In addition to Yggdrasil, there is another backup system named BOB with an IP address of 10.0.1.23. The disc space on Yggdrasil was no longer sufficient and therefore another backup system was added. Furthermore, having two backup stations increased the level of security.

In addition, the problem of domain connections discussed in subchapter 5.2 is now almost completely removed. With sites belonging to the same core network, the domain profiles and rules are validated easier and faster. As most of the devices are connected to the domain all the time, the disabling of accounts takes place right away, as well as changes in the access rights. The domain connections increased the information security level, as it is easier to control that unauthorized access is denied.

Finally, as discussed earlier in subchapter 6.4 the SSL VPN Junos Pulse connects automatically when connected to the Internet in places where VPN is needed. This means it recognizes when the user is in a domain area and does not need a VPN connection, and when the user is outside the domain area and needs a VPN connection. This is a user-friendly solution and is a benefit of the alteration of the network infrastructure.

7.2 Problems after the alteration

One of the problems was the inadequate preparedness on the firewall regulations, which resulted in problems. Some ports had to be opened after the alteration and once the virtual firewall was already in use. Table 2 illustrates the regulations and the corresponding ports that had not been properly taken into consideration during the planning phase.

Table 2. Firewall regulations and ports that had to be opened

Regulation	Port
SMTP	25
IMAP	143
POP	110
MYSQL	3306

The ports were noticed to be closed after an error. The SMTP port was noticed to be closed after ASY stopped sending reports. At the same time it was found out that if SMTP is closed, as a result POP is probably also closed. This in fact was true. IMAP was found out to be closed once a user informed that the email of another company was not working while using the WLAN at the head office. Finally, MYSQL port was noticed after an unsuccessful connection to a database of the mine software in Elijärvi that uses port 3306 as a communication channel.

A short while after switching the in-house firewall to the virtual firewall, it was noticed that the Internet connection was not working. While using the command *ping* from Röyttä in order to test the connection to the head office C, it was noticed that respond was occasional and therefore a phone call to Sonera was dialed. After a while of testing it turned out that Sonera had configured their DNS server as the primary DNS server and Apollo DNS server was not configured properly. This led to the domain name system not working. The primary DNS server was changed to Apollo at 10.0.1.11 and the secondary DNS server to Soneras' server at 193.210.18.18.

7.3 Disadvantage

A disadvantage of the outsourcing of the firewall was the firewall reporting. Having the firewall in-house enabled accurate real time reporting of network traffic and online users. The ICT department was able to manage the traffic on a packet level. Sonera offers reporting as an additional service and discussions of buying it has been going on. However, the reporting would not be as accurate as it was with Kerberos, which is the reason the additional service is not yet in use.

7.4 Infrastructural alteration on a site

The research has already explored the alteration of the network infrastructure on a WAN level, and on a LAN level at the head office C where the main changes occurred. However, some changes occurred on a site level LAN too. The head office B is used as an example of a site as it is the smallest one and easy to illustrate with in an understandable way. Other sites differ from head office B mainly by the number of end users and devices. As was discussed in subchapter 5.1, the ICT department and the Human Resources department are located in the head office B. The ICT department consists of the ICT manager and the ICT coordinator, and the Human Resources department consists of HR generalist and HR coordinator. The LAN infrastructure at the head office B before the alteration is shown in figure 11.

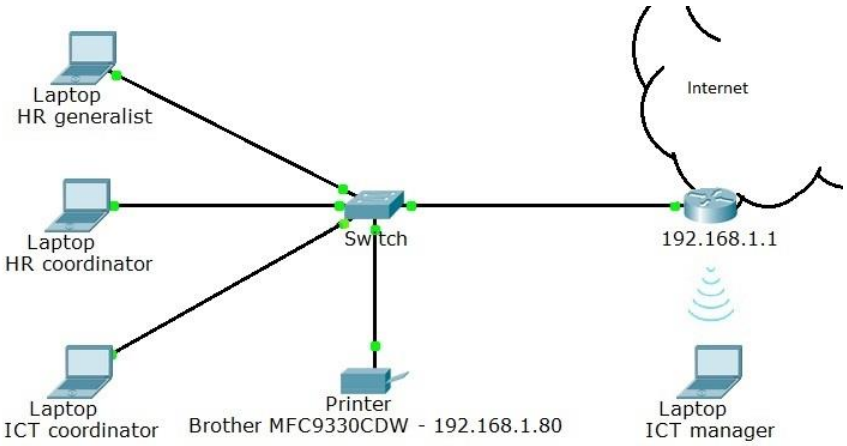

Figure 11. Head office B LAN infrastructure before the alteration

The network was 192.168.1.0 with a Huawei B593S consumer level router and Sonera consumer level 4G connection. The office had one printer, Brother MFC9330CDW with a fixed IP address of 192.168.1.80. The end users used DHCP pool. The ICT manager had an own room and was connected wirelessly to the router. The ICT coordinator and the HR department sat in the same room and were connected to a switch through a network cable, which was then connected to the router.

Today, the office belongs to the same network with head office C and uses subnetwork 10.0.3.0/24. Figure 12 illustrate the LAN infrastructure of head office B after the alteration of the network infrastructure.

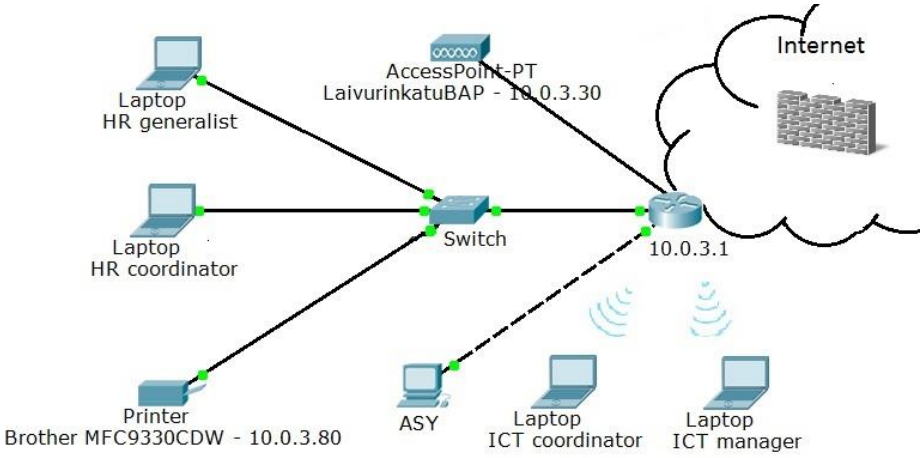

Figure 12. Head office B LAN infrastructure after the alteration

The virtual firewall in the Internet is used. The printers' address changed to 10.0.3.80, but the end users still use the DHCP pool. The ICT department is now located in one room and both the ICT manager and the ICT coordinator are connected wirelessly to the router. HR department is located in the other room and the end users are still connected to the switch through a network cable. One access point was located at the head office B with an IP address of 10.0.3.30. In addition, the automatic system ASY was moved from head office C to head office B. Both the original LAN infrastructure and the LAN infrastructure today uses star topology where the router is the central controller of the logical LAN topology.

8 SECURITY OF THE NETWORK

The level of information security and capacity increased because of the alteration. As was discussed in chapter 3, an effective data communication network has four important characteristics: delivery, accuracy, timeliness, and jitter. The case company uses star topology, which ensures the data is received by the correct destination device, and no other device. The security characteristics that are discussed later on this chapter ensures accuracy of the data. The high transmission speed of the network ensure the timeliness of the data. Finally, the up to date software and hardware ensures there is no jitter. Therefore, the case company has an effective network solution. Furthermore, as was discussed in chapter 3, the capabilities of the hardware influence the performance of the network. The original network was exceeding its capacity, which resulted in decreased performance. Today, the problem of exceeding hardware capacity has been solved by virtualizing the firewall and Tapojärvi Oy's network has high performance. Access control, trained personnel and backups ensure the reliability of the network. The backups ensure continuity of the network and hence, the business operation. Furthermore, as was discussed in subchapter 7.1, Tapojärvi Oy's ICT department is no longer the sole administrator of the firewall and hence, any problems with the firewall are quickly noticed and repaired. This quick reaction to errors offers a higher reliability of the network. The firewall, antivirus programs, and information security ensure the security of the network. Information security is achieved by network security controls and by applying the CIA triad. How confidentiality, integrity, and availability of information is secured is discussed in detail later in this chapter.

Another factor that increased security was the change from PPTP and IPSEC to SSL as SSL is more secure than PPTP and IPSEC. Furthermore, as was discussed in 6.3, the certificate for VPN authentication was installed on the local user account, meaning that only that user is able to use the VPN connection, and the user is able to use it only on that particular device. In addition, AP security increased through secure corporate level devices and the controller Hercules. In

addition, AP security consists of encryption, authentication, as well as modifying the default values and monitoring the traffic.

The ICT department is the only one that has access to the servers. The data on the servers, however, is accessible to employees as well. To keep the information secure, the access rights are very limited and each user is allowed to access only the information they need. The goal for this is to prevent unauthorized disclosure of information. In other words, the goal is to preserve confidentiality, as was discussed in subchapter 4.1. Before the alteration, modifications of access rights were not documented and rights were given too easily. Today, the access rights are automatically documented as the users have to fill a request form in which they specify where they need to gain access and why.

As was discussed in subchapter 4.2, integrity reflects the level to which information represents reality. From the integrity point of view, the network is secured by preventing unauthorized access. More importantly, the integrity is secured by having trained, professional personnel. Acceptable use policies, user access rights and security guidelines of locking computers when leaving them, as well as keeping the computers in a physically secure place achieve integrity. If needed, undesirable modifications of data can be undone by restoring backups that are run on regular intervals.

As it comes to availability, as discussed in subchapter 4.3, the data has to be accessible and usable upon demand. As it was discussed in more detail in the subchapter 5.2, most of the employees work outside the office. In addition, there are several employees travelling and therefore need to have remote access to servers. To ensure availability for remote users, the users are allowed VPN access to server. To prevent availability threats, UPS protect the servers from power loss and the hardware are constantly checked, maintained, and located properly in a physical location with air conditioning and proper locks. Finally, as mentioned earlier, backups are regularly run.

In addition, audit logs are regularly viewed and antivirus programs protect all computers. The ICT department uses the antivirus manager console to monitor the alerts and status of virus protection on devices. More importantly, end users are regularly instructed with security guidelines. These security guidelines include, for example, the intended use of company Internet and end devices, installation of software and hardware restrictions, denied and restricted applications and services, and the importance of physical safety. The users are instructed to keep their password secure and they are warned about social engineering, which is an act of representing oneself as a trusted source in order to gain knowledge of user's password.

To sum up, the security consists of physical safety, authentication policies, password policies, acceptable use policies, VPN policies, network maintenance procedures and in addition, business continuity planning. More importantly, the security consists of trained personnel who understand the concept of security as well as the risks concerning it. These security policies and procedures as well as preservation of confidentiality, integrity and availability ensure information security.

9 CONCLUSION

As was discussed in the introduction chapter, functioning connections to the servers are vital for the company; otherwise, there will be no profit. After the alteration of the network the WAN and LAN data communication networks and connections of Tapojärvi Oy are more reliable, more secure, and data transfer is faster. Therefore, from a business perspective, the alteration secured the business continuity by removing the connection problems and strengthening the information security.

For an alteration this big, enough time should be reserved and the process should be started well in advance. The process is demanding from the time management point of view as solely the negotiations with the co-operating partner could go on for over a year. The details have to satisfy both parties, and the price have to be agreed upon. Furthermore, the device manufacturer or delivery could delay the process. An infrastructural alteration also demands the consideration of business schedule. The schedule has to be discussed with accounting and salary calculation in order to ensure that the alteration has minimal impact on the business. Once the details, price and schedule has been agreed upon and the contracts are signed, it is only a matter of the technical implementation.

It is important to carefully plan the alteration and take into consideration all its aspects. However, it is also important to remember that even big changes such as an infrastructural alteration have to be eventually made and should not be postponed for too long. It does not matter how carefully everything is planned, there will most likely still be some aspects that was not taken into consideration. For example, something was considered a small risk but turned out to be a big one or something that was thought not to cause a problem but did. The most important aspect is to carefully mitigate big risks. Small problems are unfortunate consequences but yet manageable.

For the case company, my suggestion for further development is that once the technical specifications allow it, all sites should become part of the same core

network. In Tapojärvi Oy's network, the sites that are not yet part of the same core network are Kylylahti, Pampalo and Kittilä. Adding these sites to the same core network would decrease the number of remote users even more and increase the security level. All sites would have domain connections and all WLANs would have a centralized management. The monitoring of traffic would be possible in the entire organization.

In addition, to remove the problem that a power outage causes, i.e. loss of connection to servers, the servers should be virtualized. If the servers were virtualized, the power outage would only affect the head office and all sites could continue their operations without interruptions. The virtualization of servers should proceed in order of priority.

Alterations to network should be well managed to avoid malfunctioning of the network. Furthermore, the management of networks should include anticipation of the future. In other words, factors such as capabilities of hardware have to be considered well in advance. As Cisco, the worldwide leading company in networking once campaigned "Tomorrow starts today".

REFERENCES

Andress, J. 2014. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Waltham: Syngress.

Ciccarelli, P., Faulkner, C., FitzGerald, J., Dennis A. Groth, D. & Skandier T. 2012. Introduction to Networking Basics. Crawfordsville: John Wiley & Sons.

Coca Jr., J., Gardinier, K., Morimoto, R. & Noel, M. 2004. Microsoft Server 2003 Unleashed. Indianapolis: Sams Publishing.

Collis, J. & Hussey, R. 2009. Business Research: A Practical Guide for Undergraduate and Postgraduate Students. New York: Palgrave Macmillan.

Ellet, W. 2007. The Case Study Handbook. Boston: Harvard Business Press.

Fitzgerald, D. 2007. Business Data Communications and Networking. Crawfordsville: John Wiley & Sons.

Forouzan, B. 2007. Data Communication and Networking. New York: The McGraw-Hill companies.

Greene, S. 2006. Security Policies and Procedures Principles and Practices. Pearson Education, Inc.

ISO/IEC 2014. ISO/IEC 27000:2014(en). Online Browsing Platform (OBP). Referenced October 11, 2015. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en.

Mattord, H. & Whitman, M. 2005. Principles of Information Security. Boston: Thomson Course Technology.

Sullivan, D. 2007. The Shortcut Guide To Extended Validation SSL certificates. San Francisco: Realtime Publishers.

Tapojärvi Oy 2015. Human resource plan 2015. Referenced October 15, 2015.

Tipton, H. & Krause, M. 2008. Information Security Management Handbook. Boca Raton: Auerbach Publications Taylor & Francis Group.

Yin, R., 2009. Case Study Research Design and Methods. Thousand Oaks: SAGE publications, Inc.